Order Code RL30677

CRS Report for Congress
Received through the CRS Web

Digital Surveillance: The Communications Assistance for Law Enforcement Act

Updated May 3, 2005

Patricia Moloney Figliola
Specialist in Telecommunications and Internet Policy
Resources, Science, and Industry Division

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
03 MAY 2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Digital Surveillance: The Communications Assistance for Law Enforcement Act	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **David D. Acker Library and Knowledge Respository, Defense Acquisition University, Fort Belvoir, VA**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**16**	

Digital Surveillance: the Communications Assistance for Law Enforcement Act and FBI Internet Monitoring

Summary

The Communications Assistance for Law Enforcement Act (CALEA, P.L. 103-414, 47 USC 1001-1010), enacted October 25, 1994, is intended to preserve the ability of law enforcement officials to conduct electronic surveillance effectively and efficiently despite the deployment of new digital technologies and wireless services that have altered the character of electronic surveillance. CALEA requires telecommunications carriers to modify their equipment, facilities, and services, wherever reasonably achievable, to ensure that they are able to comply with authorized electronic surveillance actions.

The modifications, originally planned to be completed by 1998, have been delayed due to disagreements among the telecommunications industry, law enforcement agencies, and privacy rights groups, over equipment standards, and other technical issues. Disagreements over amount of federal funds to be provided to the telecommunications carriers for CALEA implementation, which carriers are eligible to receive those funds, and privacy concerns, have also impeded implementation.

After receiving petitions from the industry and the Federal Bureau of Investigation (FBI) over the dispute, the Federal Communications Commission (FCC) in 1999 ruled in favor of most of the FBI's requests. This decision resulted in lawsuits being filed by industry and privacy rights groups. In August 2000, a federal appeals court upheld parts of the FCC's decision, but remanded most of it for reconsideration. Since that time, the FCC established June 30, 2002, as the final CALEA compliance date, but it has granted numerous waivers and full CALEA implementation remains incomplete.

The FBI and other law enforcement agencies, the FCC, and Congress are all actively addressing CALEA-related concerns. On March 10, 2004, the FBI, the Department of Justice, and the Drug Enforcement Administration petitioned the FCC to identify additional telecommunications services not identified specifically within CALEA that should be subject to it. In response to the petition and after considering the comments and replies from interested parties, the FCC released an Notice of Proposed Rulemaking (NPRM) and declaratory ruling on August 4, 2004. In the NPRM, the FCC drew a number of tentative conclusions regarding CALEA applicability; addressed compliance issues; and developed a proposal for implementation costs and time frame. Comments and replies to the NPRM were due November 8 and December 7, 2004, respectively. Accompanying the NPRM was a declaratory ruling in which the FCC clarifies that commercial wireless "push-to-talk" services are subject to CALEA, regardless of the technologies that wireless providers choose to apply in offering them.

Thus far in the 109th Congress, no bills have been introduced that would amend the CALEA statute. It is possible that a bill related to Internet Protocol-enabled services may have provisions that will affect CALEA-related powers.

Contents

Background 1
Some Technical Terms 2

CALEA's Main Provisions 3

Major Events Following Enactment of CALEA 4
Initial Delays 4
The FBI's "Punch List" 5
Capacity Requirements 6
Previous FCC Actions 6

Recent Activity 9
FBI Action 9
Comments to the FCC's Wireless Broadband Task Force Report 9
Notice of Information Collection Under Review 9
Petition for Declaratory Ruling 9
Inspector General Report 9
FCC Action 10
Tentative conclusions regarding CALEA applicability 10
Compliance issues 10
Implementation costs and timeframe 11
Declaratory ruling 11
Congressional Action: 109th Congress 11
Congressional Action: 108th Congress 11
House of Representatives 11
Senate 11
Comparison of the House and Senate CALEA-related provisions . . . 12

Issues for the Congress 13

Digital Surveillance: The Communications Assistance for Law Enforcement Act

Background

In the early 1990s the Federal Bureau of Investigation (FBI) asked Congress for legislation to assist law enforcement agencies to continue conducting electronic surveillance. The FBI argued that the deployment of digital technologies in public telephone systems was making it increasingly difficult for law enforcement agencies to conduct electronic surveillance of communications over public telephone networks. As a result of these arguments and concerns from the telecommunications industry,[1] as well as issues raised by groups advocating protection of privacy rights,[2] the Communications Assistance for Law Enforcement Act (CALEA) was enacted on October 25, 1994 (47 USC 1001-1021), in the final days of the 103rd Congress.

CALEA is intended to preserve the ability of law enforcement officials to conduct electronic surveillance effectively and efficiently, despite the deployment of new digital technologies and wireless services by the telecommunications industry. CALEA requires telecommunications carriers to modify their equipment, facilities, and services to ensure that they are able to comply with authorized electronic surveillance. These modifications were originally planned to be completed by October 25, 1998. Since that time, the Federal Communications Commission (FCC) issued two additional orders establishing June 30, 2002, as the date by which telecommunications carries must have upgraded all their systems.[3] Equipment manufacturers have fulfilled their obligation to provide CALEA solutions and carriers are implementing them. The FBI and FCC continue to monitor and review the implementation of this program.

---

[1] In this report, the telecommunications industry includes common carrier telephone companies, mobile wireless telecommunications providers, telecommunications equipment manufacturers, and other entities that provide telecommunications services to the public.

[2] Privacy rights groups involved in the CALEA debate include the Electronic Privacy Information Center, the Electronic Frontier Foundation, advocacy groups which both support on-line privacy rights of individuals, the Center for Democracy and Technology, which also advocates electronic privacy (and is funded primarily by the telecommunications, computer, and media industries), and the American Civil Liberties Union (ACLU), which represents a broad array of civil rights based on the First and Fourth Amendments.

[3] United States Department of Justice, Federal Bureau of Investigation, *Communications Assistance for Law Enforcement Act, Eighth Annual Report to Congress*, November 30, 2002 (*Eighth Annual Report*), pp. 7-9.

Some Technical Terms

As a result of the revolution in digital technology in telecommunications, the process of wiretapping and other electronic surveillance has become more complex, and legal ambiguities have been introduced. As a background to understanding the problems associated with CALEA implementation, the definitions of several terms are necessary. Electronic surveillance refers to either the interception of communications content (as in a conversation) also known as wiretapping, or the acquisition of call-identifying information (the number dialed). The latter activity is accomplished through the use of pen register devices, which capture call-identifying information for numbers of outgoing calls from the location of lawful interception, and traps and traces, which capture information for numbers received at the location of lawful interception, much like consumer caller ID systems. Under current federal law, law enforcement (i.e., police or the FBI) must obtain a court order before conducting any of these activities. However, a wiretap requires a higher "evidentiary burden" than a pen register or trap and trace, including showing that there is probable cause for believing that a person is committing one of a list of specific crimes.[4]

Under traditional analog technology, it was easy to separate the above categories of electronic surveillance. However, the advent of digital signal transmission technologies has made that distinction less clear. Information signals (voice or data) can be transmitted over telephone networks in one of two ways: circuit-switched and packet-switched modes.[5] In circuit-switched systems, a communications path is established between the parties and dedicated exclusively to one conversation for the duration of the call. In packet-switched systems, the information is broken down into smaller pieces called "packets"using a digital process. Each packet contains a small part of the message content along with call-identifying information called a "header" that indicates the origination and destination points of the information. Each packet is transmitted separately and is reassembled into the complete message at the destination point.

The packet-switched mode is the signal transmission technology used in all Internet communications. Packet switching is considered a more efficient use of a network than circuit switching because the same line can be used for multiple communications simultaneously. Although the circuit-switched mode was historically used in all voice telephone calls, the packet-switched mode is increasingly being used for voice and data transmissions over telephone networks.

---

[4] See CRS Report 98-326 A, *Taps, Bugs & Telephony: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, March 23, 1998.

[5] Switches are network devices that select a path or circuit for sending data to its next destination over the telephone network. Switches may also include functions of the router, a device also used in computer networks, that determines the route and adjacent network point for data to be sent.

CALEA's Main Provisions

CALEA requires telecommunications carriers to assist law enforcement in performing electronic surveillance on their digital networks pursuant to court order or other lawful authorization. The telecommunications industry, privacy rights groups, and law enforcement agencies agree that CALEA was not intended to expand law enforcement's authority to conduct electronic surveillance. On the contrary, CALEA was intended only to ensure that after law enforcement obtains the appropriate legal authority, carriers will have the necessary capabilities and sufficient capacity to assist law enforcement in conducting digital electronic surveillance regardless of the specific telecommunications systems or services deployed.

CALEA (47 USC 1002) directs the telecommunications industry to design, develop, and deploy solutions that meet certain assistance capability requirements for telecommunications carriers to support law enforcement in the conduct of lawfully-authorized electronic surveillance. Pursuant to a court order or other lawful authorization, carriers must be able, within certain limitations, to: (1) expeditiously isolate all wire and electronic communications of a target transmitted by the carrier within its service area; (2) expeditiously isolate call-identifying information that is reasonably available on a target; (3) provide intercepted communications and call-identifying information to law enforcement; and (4) carry out intercepts unobtrusively, so targets are not made aware of the electronic surveillance, and in a manner that does not compromise the privacy and security of other communications.

To allow carriers to give law enforcement the means to conduct its wiretaps, CALEA (47 USC 1003) requires the Attorney General to determine the number of simultaneous interceptions (law enforcement agencies' estimate of their *maximum capacity* requirements) that telecommunications carriers must be able to support.

To maintain privacy rights of individuals, CALEA (47 USC 1004) requires telecommunications carriers to ensure that any interception of communications or access to call-identifying information that is conducted within their premises can only be done with a court order. It also requires the specific intervention of an officer or employee of the carrier acting in accordance with regulations prescribed by the Federal Communications Commission (FCC).

CALEA (47 USC 1005) directs telecommunications carriers to consult with telecommunications equipment manufacturers to develop equipment necessary to comply with the capability and capacity requirements identified by the FBI. For efficient industry-wide implementation of the above requirements, CALEA (47 USC 1006) directs the law enforcement community to coordinate with the telecommunications industry and state utility commissions to develop suitable technical standards and establish compliance dates for equipment. In its *Eighth Annual Report*, the FBI stated that, "to date, most manufacturers have either complete, or nearly complete, CALEA solutions available for their carrier customers."[6]

---

[6] Eighth Annual Report, p. 5.

CALEA (47 USC 1008) gives the Attorney General, subject to the availability of appropriations, authority to pay telecommunications carriers for all reasonable costs directly associated with the modifications performed by carriers in connection with equipment, facilities, and services installed or deployed on or before January 1, 1995 (known as the "grandfather" date).

Major Events Following Enactment of CALEA

Initial Delays

CALEA gave implementation responsibility to the Attorney General, who, in turn, delegated the responsibility to the FBI. The FBI leads that nationwide effort on behalf of federal, state, and local law enforcement agencies. FBI officials initially anticipated that it would take a year for a standard to be developed and agreed upon by law enforcement, the telecommunications carriers, and the equipment manufacturers. Telecommunications consultants estimated that it would take the industry another three years to design, build and deploy new systems to comply with CALEA. Instead, industry and law enforcement became involved in a protracted dispute over what should be required for law enforcement's wiretapping capabilities.

By March 1997, the completion of the capability standard was overdue by 16 months. The FBI attempted to expedite the industry's implementation of CALEA by releasing regulations that included a cost recovery plan for the federal government's payment of costs associated with CALEA, as well as capability and capacity requirements for the industry to meet. The plan required more extensive upgrades to networks than the telecommunications industry believed were necessary for law enforcement to preserve its wiretapping capabilities. Industry groups and privacy advocates disputed the FBI's plan. They argued that the FBI was attempting to expand its surveillance capabilities beyond the congressional intention of CALEA, and was attempting to unfairly shift costs and accountability away from the federal government onto private industry. Furthermore, the industry argued that, without an adopted capability standard, it could not begin designing, manufacturing, and purchasing the equipment to achieve CALEA compliance.

In December 1997, the Telecommunications Industry Association (TIA, representing telecommunications equipment manufacturers) adopted, over the objections of the law enforcement community, a technical standard, J-STD-025, also known as the "J-standard." This standard prescribes upgrades to network devices to meet CALEA's assistance capability requirements for local exchange, cellular, and broadband personal communications services (PCS). Although the FBI claimed that the J-standard did not provide all of the capabilities needed, the industry asserted that CALEA's language stated that telecommunications carriers would be compliant if they met publicly available standards adopted by the industry.

Privacy rights groups, on the other hand, protested two aspects of the J-standard that they asserted would make information beyond what is legally required available to law enforcement. One was a feature enabling the telecommunications network to provide location information for users of mobile wireless telecommunications services. The location information protocols in J-STD-025 allow law enforcement

agencies to obtain information on the physical location of the nearest cell site (i.e., the receiver/transmitter antenna and base station) of mobile phone handsets at the beginning and end of each call. Wireless carriers are now deploying another technology (called triangulation) that will enable the carriers, and law enforcement, to track wireless telephone users more precisely, potentially within a few meters. The other was a feature enabling the network to access packet-mode data from telephone calls using more advanced systems. Privacy rights groups argued that these capabilities would violate the Fourth Amendment rights of individuals against unreasonable searches and seizures. Despite these objections, telecommunications manufacturers began designing new switches and upgrades to existing switches according to the J-standard.

Currently, equipment manufacturers have successfully incorporated the J-standard into their new equipment and carriers are now well underway with their efforts to upgrade their systems.

The FBI's "Punch List"

In the negotiations to develop the J-standard, TIA had refused to include some of the capabilities that law enforcement officials claimed they needed to facilitate digital wiretapping. As a result, in March 1998, the FBI petitioned the FCC to require the telecommunications industry to adopt eleven additional capabilities. Industry and privacy rights groups protested that the FBI's plan would unlawfully expand enforcement capabilities. Eventually, the "punch-list"[7] included the following six[8] items:

- Content of subject-initiated conference calls -- Would enable law enforcement to access the content of conference calls supported by the subject's service (including the call content of parties on hold).
- Party hold, join, drop -- Messages would be sent to law enforcement that identify the active parties of a call. Specifically, on a conference call, these messages would indicate whether a party is on hold, has joined or has been dropped from the conference call.
- Subject-initiated dialing and signaling information -- Access to all dialing and signaling information available from the subject would inform law enforcement of a subject's use of features (such as the use of flash-hook and other feature keys).
- In-band and out-of-band signaling (notification message) -- A message would be sent to law enforcement whenever a subject's *service* sends a tone or other network message to the subject or associate (e.g., notification that a line is ringing or busy).

---

[7] The "punch list" was named as such by the telecommunications industry, which believed the FBI was improperly forcing industry to comply with the FBI's requirements.

[8] The additional capabilities originally requested by the FBI that were not included were: standardized delivery interface; separated delivery, surveillance status; continuity check tone (c-tone); and feature status.

- Timing information -- Information necessary to correlate call-identifying information with the call content of a communications interception.
- Dialed digit extraction -- Information would include those digits dialed by a subject after the initial call setup is completed.[9]

Capacity Requirements

The FBI's subsequent implementation actions were also opposed by the telecommunications industry. In March 1998, the FBI announced its estimated capacity requirements for local exchange, cellular, and broadband PCS.[10] The industry protested the FBI's estimates, arguing that it would require telephone carriers to accommodate thousands of wiretaps simultaneously, an impractical and unnecessary burden. In July 1998, the FBI developed guidelines and procedures to facilitate small carrier compliance with its capacity requirements, and asked carriers to identify any systems or services that did not have the capacity to accommodate those requirements. In December 1998, the FBI began a proceeding to develop capacity requirements for services other than local exchange, cellular, and broadband PCS, asked additional questions of interested parties in June 2000.[11] These technologies and services included paging, mobile satellite services, specialized mobile radio, and enhanced specialized mobile radio. To date, the proceeding is still pending.

Previous FCC Actions

As a result of petitions from the industry and the FBI, the FCC became involved in the implementation of CALEA. In October 1997, the FCC released its first Notice of Proposed Rule Making (NPRM) on CALEA implementation.[12] The NPRM sought comments from interested parties regarding a set of policies and procedures proposed by the FCC for telecommunications carriers to follow. The proposed procedures would (1) preclude the unlawful interception of communications, (2) ensure that authorized interceptions are performed, (3) maintain secure and adequate records of any interceptions, and (4) determine what entities should be subject to these requirements, whether the requirements are reasonable, and whether to grant extensions of time for compliance with the requirements.

In response to the NPRM, telecommunications carriers, privacy rights groups, and the FBI submitted comments to the FCC to attempt to influence the final decision. Then, in April 1998, the FCC released a Public Notice requesting comments on issues raised in those petitions concerning the dates that carriers were required to comply with CALEA and the dispute over the J-standard. Based on

---

[9] Federal Register 63 page 63639, FCC, Further Notice of Proposed Rulemaking, November 16, 1998.

[10] Federal Register 63, page 12217, FBI, Final Notice of Capacity, March 12, 1998.

[11] Federal Register 63, page 70160, FBI Notice of Inquiry, December 18, 1998, and Federal Register 65, page 40694, FBI Further Notice of Inquiry, June 30, 2000.

[12] FCC NPRM CC Docket No. 97-213, FCC Record 97-356, released October 10, 1997.

comments it received, the FCC extended the implementation deadline until June 30, 2000, stating that without a standard, the necessary equipment would not be available in time.[13]

In October 1998, the FCC initiated a proceeding to review the technical capabilities prescribed by the J-standard.[14] The goal of that proceeding was to determine whether telecommunications carriers should be required under CALEA to meet the FBI's "punch list" items. The FCC addressed these issues in several documents released over the following year. In March 1999, the FCC's First Report and Order established the minimum capability requirements for telecommunications carriers to comply with CALEA.[15] Telecommunications carriers were required to ensure that only lawful wiretaps occur on their premises and that the occurrence of wiretaps is not divulged to anyone other than authorized law enforcement personnel. On August 2, 1999, the FCC decided to allow carriers to decide how long they would maintain their records of law enforcement's wiretap, pen register, and trap and trace interceptions.[16] On August 31, 1999, the Second Report and Order established a definition for "telecommunications carrier" to include all common carriers, cable operators, electric and other utilities that offer telecommunications services to the public, commercial mobile radio services, and service resellers.[17] The definition did not include Internet service providers (ISPs), which were explicitly excluded under the CALEA statute.

The FCC's Third Report and Order, released August 31, 1999, adopted technical requirements for wireline, cellular, and broadband PCS carriers to comply with CALEA requirements.[18] The ruling adopted the J-standard, including the two capabilities that were opposed by the privacy rights groups (i.e., the ability to provide location information and packet-mode data to law enforcement). As described above, the FCC also adopted six of the punch list capabilities requested by the FBI to be implemented by telecommunications carriers. The Order required all aspects of the J-standard except for the packet-mode data collection capability to be implemented by June 30, 2000. The Order required carriers to comply with the packet-mode data capability and the six punch list capabilities by September 30, 2001.[19] (The FCC

---

[13] FCC Memorandum Opinion and Order in the Matter of Petition for the Extension of the Compliance Date under Section 107 of CALEA, released September 11, 1998.

[14] FCC Proposes Rules to Meet Technical Requirements of CALEA. Report No. ET 98-8. FCC News, October 22, 1998.

[15] FCC 99-11, Report and Order CC Docket No. 97-213, released March 15, 1999.

[16] FCC 99-184, Order on Reconsideration, CC Docket No. 97-213, released August 2, 1999.

[17] FCC 99-229, Second Report and Order, CC Docket No. 97-213, released August 31, 1999.

[18] FCC 99-230, Third Report and Order, CC Docket No. 97-213, released August 31, 1999.

[19] FCC Sides with FBI on Tapping, *Wired News*, August 27, 1999, [http://www.wired.com/news].

ultimately extended the date by which all telecommunications carriers must have upgraded their systems to June 30, 2002.[20])

On April 9, 2001, the FCC adopted its Second Order on Reconsideration,[21] which clarified the arrangements telecommunications carriers must make to ensure that law enforcement agencies can contact them when necessary, and the interception activity that triggers a record-keeping requirement.

In September 2001, FCC released a tandem Order[22] and Public Notice[23] on CALEA implementation. In the Order, the Commission extended until November 19, 2001, the deadline by which wireline, cellular, and broadband personal communications services (PCS) carriers must implement a packet-mode communications electronic surveillance capability, or to seek individual relief under section 107(c) of CALEA. The notice explained the petitioning process for telecommunications carriers seeking relief under section 107(c) for an extension of the new compliance deadline with respect to packet-mode communications, as well as other safe harbor standards.

Finally, on April 11, 2002, the FCC released an Order on Remand,[24] which responded to a decision issued by the United States Court of Appeals for the District of Columbia Circuit[25] vacating four of the punch list electronic surveillance capabilities mandated by the Third Report and Order in this proceeding. The FCC found that all of the capabilities were necessary and authorized by CALEA and had to be provided by wireline, cellular, and broadband PCS telecommunications carriers by June 30, 2002. The FCC also required that two additional punch list capabilities that were mandated by the Third Report and Order, but not reviewed by the Court of Appeals be provided by that same date.

The FCC granted preliminary extensions to requesting carriers with respect to punch list implementation that will expire on June 30, 2004. It granted preliminary extensions in connection with "packet" services that had been scheduled to expire on November 19, 2003, but that date was further extended to January 30, 2004. No further action with respect to that extension has been taken.

---

[20] FCC Pubic Notice DA 02-270, released March 26, 2002.

[21] Federal Register 66, page 22446, FCC, Second Order on Reconsideration, CC Docket No. 97-213, May 4, 2001.

[22] Federal Register 66, page 50841, FCC, Order, CC Docket No. 97-213, October 5, 2001.

[23] FCC Pubic Notice DA 01-2243, released September 28, 2001.

[24] Federal Register 67, page 21999, Order on Remand, CC Docket No. 97-213, May 2, 2002.

[25] See United States Telecom. Association v. FCC, 227 F.3d 450 (D.C. Cir. 2000), available at [http://www.fcc.gov/ogc/documents/opinions/2000/99-1442.html].

Recent Activity

The FBI and other law enforcement agencies, the FCC, and Congress are all concerned with CALEA-related issues, particularly with respect to packet-based services (i.e., voice over Internet Protocol [VoIP]) and "push-to-talk" services offered by wireless providers.

FBI Action

The FBI has remained active in promoting its positions related to CALEA related powers.

Comments to the FCC's Wireless Broadband Task Force Report. On April 22, 2005, the DOJ filed comments on the FCC's Wireless Broadband Task Force Report,[26] requesting that the FCC "continue to preserve the vital national security and criminal law enforcement capabilities of CALEA as it develops a deregulatory framework for wireless broadband Internet access services." Reply comments in the proceeding are due May 23, 2005.

Notice of Information Collection Under Review . On April 13, 2005, the FBI published a 60-day Notice of Information Collection Under Review.[27] The notice announces a CALEA Readiness Survey program, which seeks to evaluate the effectiveness of CIU programs for implementing CALEA solutions in the Public Switched Telephone Network. Comments will be accepted until June 13, 2005.

Petition for Declaratory Ruling. On March 10, 2004, the FBI, the Department of Justice, and the Drug Enforcement Administration petitioned the FCC to identify additional telecommunications services not identified specifically within CALEA that should be subject to it.[28] The services named in the FBI petition include some now considered beyond the scope of CALEA by many observers, including services that fall under the FCC's definition of "information services" under the Communications Act of 1934. The FBI believes that CALEA gives the FCC a broader framework to determine that a service is a "telecommunications service." Comments and replies to the petition were due April 12 and April 27, 2004, respectively.

Inspector General Report. The FBI's Inspector General issued a report in April 2004 on CALEA implementation.[29] In its report, the IG expressed concern

---

[26] GN Docket No. 04-163. Additional information on this topic can be found online at the FCC's website at [http://www.fcc.gov/wbatf].

[27] 70 Fed. Reg. 19,503 (2005). This document is available online at [http://www.askcalea.net/docs/20050413_70fr19503.pdf].

[28] Joint Petition for Expedited Rulemaking of United States Department of Justice, Federal Bureau of Investigation, and Drug Enforcement Administration, RM-10865, March 10, 2004.

[29] U.S. Department of Justice, Office of the Inspector General of the, entitled

(continued...)

over the cost estimates for obtaining CALEA compliance, which have varied widely. Industry has stated it believes estimates full compliance will cost approximately $1.3 billion; the FBI has estimated costs in the range of $500 million to $1 billion. Further, in December 2003, the FBI estimated that an additional $204 million would be necessary to complete deployment of CALEA. The IG stated in its report that it did not believe implementation costs could be determined with any degree of specificity, but that it was unlikely CALEA could be implemented with the $49.5 million that remains unobligated from current funding.

FCC Action

In response to the petition and after considering the comments and replies from interested parties, the FCC released an NPRM and declaratory ruling on August 4, 2004.[30] Comments and replies to the NPRM were due November 8 and December 7, 2004, respectively. It is anticipated that the FCC will issue its report during the second quarter of 2005.

Tentative conclusions regarding CALEA applicability. In the NPRM, the FCC tentatively concluded that CALEA applies to facilities-based providers of any type of broadband Internet access service – including wireline, cable modem, satellite, wireless, and powerline – and to managed or mediated VoIP services. These tentative conclusions are based on an FCC proposal that these services fall under CALEA as "a replacement for a substantial portion of the local telephone exchange service." Additionally, the FCC tentatively concluded that it is unnecessary to identify future services and entities subject to CALEA. The FCC stated that it recognized law enforcement's need for certainty in this area, but that it anticipated that the report and would resolve law enforcement's and industry's uncertainty about future compliance obligations.

Compliance issues. The FCC requested comments on telecommunications carriers' obligations and compliance solutions as they relate to broadband Internet access and VoIP. In particular, the FCC requested comments on the feasibility of carriers relying on a trusted third party to manage their CALEA obligations and whether standards for packet-mode technologies are deficient and thus preclude carriers from relying on them as safe harbors for complying with CALEA.

The FCC also proposed mechanisms to ensure that telecommunications carriers comply with CALEA. Specifically, the FCC proposed to restrict the availability of compliance extensions and clarifies which carriers may be reimbursed for their

---

[29] (...continued)
"Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation," available at [http://www.usdoj.gov/oig/audit/FBI/0419/final.pdf], April 7, 2004.

[30] *In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services, Notice of Proposed Rulemaking and Declaratory Ruling*, FCC 04-187, ET Docket 04-295, RM-10865, adopted August 4, 2004, released August 9, 2004. Available online at [http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-187A1.pdf]. See also Federal Register 69, page 56976.

CALEA compliance costs. The FCC proposed to afford all carriers with pending petitions a reasonable period of time (e.g., 90 days) in which to comply with, or seek relief from, any determinations that it eventually adopts.

Additionally, the FCC considered whether, in addition to the enforcement remedies through the courts available to law enforcement, it may take separate enforcement action against carriers that fail to comply with CALEA. The FCC tentatively concluded that it has general authority to promulgate and enforce CALEA rules.

Implementation costs and timeframe. The FCC tentatively concluded that carriers are responsible for CALEA development and implementation costs for post-January 1, 1995 equipment and facilities and sought comment on a variety of cost recovery issues.

Declaratory ruling. In the companion declaratory ruling, the FCC clarified that commercial wireless "push-to-talk" services are subject to CALEA, regardless of the technologies that wireless providers choose to apply in offering them.

Congressional Action: 109th Congress

Thus far in the 109th Congress, no bills have been introduced that would amend the CALEA statute. It is possible that a bill related to Internet Protocol-enabled services may have provisions that will affect CALEA-related powers.

Congressional Action: 108th Congress

Two bills were introduced in the 108th Congress that would have had an impact on CALEA-related powers for law enforcement, although neither would have actually amended the CALEA statute.

House of Representatives. In the House of Representatives, H.R. 4129, the VOIP Regulatory Freedom Act of 2004, was introduced by Representative Pickering on April 2, 2004, and referred to the Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet on April 8, 2004.[31] The subcommittee also held a hearing on September 8, 2004, "Law Enforcement Access to Communications in a Digital Age." Although that hearing was not held specifically to address H.R. 4129, it did touch on many of the implementation issues that are facing service providers and law enforcement.[32]

Senate. In the Senate, S. 2281, the VOIP Regulatory Freedom Act of 2004, was introduced and referred to the Committee on Commerce, Science, and

---

[31] The VOIP Regulatory Freedom Act of 2004, H.R. 4129, Section 4 (c)(1)-(3).

[32] The House held other hearings during the 108th Congress that addressed telecommunications and Internet-related issues. A full list of the hearings held by the Committee on Energy and Commerce is available online at [http://energycommerce.house.gov/108/action.htm].

Transportation by Senator Sununu on April 5, 2004. This bill was intended as a companion bill to H.R. 4757, the Advanced Internet Communications Services Act of 2004, although H.R. 4757 did not contain any CALEA-related provisions.

A hearing on S. 2281 was held by the Committee on Commerce, Science, and Transportation on June 16, 2004,[33] and the bill was ordered to be reported with an amendment in the nature of a substitute favorably on July 22, 2004; the substitute language was significantly different than that in the original bill. On November 19, 2004, the bill was again reported by Senator McCain and placed on the Senate Legislative Calendar, first without written a report on November 19, 2004, and then with a written report on December 7, 2004 (see S.Rept. 108-425).

Comparison of the House and Senate CALEA-related provisions. Neither bill would have amended CALEA – each provided its own statutory requirements separate from CALEA. However, the House bill contained much more specific language than the Senate bill, which only stated that the FCC "shall require a provider of a connected VoIP application to provide access to necessary information to law enforcement agencies not less than that require of information service providers."[34] A "connected VoIP application" is defined in both bills as "a VoIP application that is capable of receiving voice communications from or sending voice communications to the public switched network, or both."

The House bill, which was seen as much more favorable to law enforcement interests than the Senate bill, would have required the FCC to conduct a proceeding within 180 days of the date of enactment to "determine whether it is technologically feasible and reasonable" to apply the assistance capability requirements now applied to the "equipments, facilities, or services of a telecommunications carrier" to a connected VoIP application.[35] If the FCC were to have made an affirmative determination in this case, it would have be required to establish "rules, technical requirements, and standards" to apply such requirements while also protecting privacy and security, minimizing the costs of implementation, continuing to encourage the development of new technologies, and providing a reasonable time for compliance. In developing these rules, the FCC would have been required to consult with affected service providers, equipment manufacturers, the U.S. Attorney General, state and local law enforcement, and other interested parties.[36]

---

[33] The Senate held other hearings during the 108th Congress that addressed telecommunications and Internet-related issues. A full list of the hearings held by the Committee on Commerce, Science, and Transportation is available online at [http://commerce.senate.gov/hearings/index.cfm].

[34] The VOIP Regulatory Freedom Act of 2004, S. 2281, Section 4 (c).

[35] The bill would also require the FCC to undertake such a proceeding every six months until such time as a determination is made.

[36] See also Tech Law Journal, "Summary of VOIP Related Bills," July 21-25, 2004. Available online at [http://www.techlawjournal.com/home/newsbriefs/2004/07e.asp]. This article also contains a comparison of the non-CALEA-related provisions of these bills.

Issues for the Congress

A number of issues exist that Congress may wish to consider as it addresses concerns related to CALEA implementation:

- The FCC has been examining a number of issues related to new technologies that could affect CALEA (e.g., VoIP[37], Broadband over Powerlines[38]). What impact might these new technologies have on the way CALEA is implemented and enforced?

- Will it be necessary to amend CALEA to keep up with advances and changes in technology and, if so, how? Would previous legislative proposals (H.R. 4129 and S. 2281) have pre-empted the need to amend CALEA? How could the FCC's rulemaking in response to the FBI petition affect service and application development and deployment?

- Might it be possible for law enforcement to expand the reach of CALEA without additional legislative action? If so, how should privacy rights be balanced against such new applications of the law?

- The DOJ IG does not believe the remaining Telecommunications Carrier Compliance Fund is sufficient to pay for the remaining equipment upgrades that are needed for all carriers to be compliant with CALEA. How could this potential shortfall be mitigated?

---

[37] See the FCC's VOIP page for additional information, [http://www.fcc.gov/voip/]. See *In theMatter of IP-Enabled Services, Notice of Proposed Rulemaking*, FCC 04-28, WC Docket 04-36, adopted February 12, 2004, released March 10, 2004. Available online at [http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-28A1.pdf].

[38] See *Inquiry Regarding Carrier Current Systems, including Broadband over Powerline Systems, Notice of Proposed Rulemaking*, FCC 04-29, ET Docket 03-104, adopted February 12, 2004, released February 23, 2004. Available online at [http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-29A1.pdf].